Bring-your-owndevice (BYOD) can increase your risk of cyber threats.

As remote and hybrid work become the norm, businesses face new security challenges. With the increased use of both company-owned and personal devices (BYOD), and the flexibility to work from anywhere - from the office to home or a local coffee shop - the number of potential access points for cybercriminals is increasing.

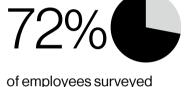




employees to access email on personal phones/tablets.1

41% permitted employees to use

personal phones/tablets for accessing corporate systems and data (BYOD).1



use personal devices for work activities.1

The hidden dangers of a mobile workforce.

When employees use their own smartphones for work related activity, such as messaging using consumer apps or accessing corporate files over a public Wi-Fi connection, your company can be exposed to significant risks:

54% Users were almost twice

as likely to click on a phishing link on a personal device (54.2%) as a company-owned one (27.5%).2

of personal devices were

exposed to a mobile phishing attack in 2022.3 51% of organization have

experienced mobile app-related incidents from factors such as malware or unpatched vulnerabilities.4

How threat actors leverage mobile devices:



Threat actors unlock the

operating system, bypassing

Jailbreak

security features to load malware and intercept communications.



stealing credentials, and send emails or messages.

impersonate the user by

connected network,

Hijack



Attackers use email, SMS or phone calls to lure

individuals into clicking malicious links or providing personal information.

\$9.36m

The cost of a data breach.

the average total cost of a data breach for organizations in the US in 2024, the highest among the 16 countries and

regions studied.

the global average cost of a data breach for organizations in 2024, a 10% increase from

\$4.88m

the pandemic.5

2023 - the biggest jump since

businesses said they would face financial and/or regulatory penalties if

shared on a mobile device in an unsecure way.6

sensitive information were

Take back control.

By switching your mobile device policy from BYOD to company managed, you gain control over your applications, content and data. Owning and managing employee devices lets you update and respond to the latest threats quickly, helping reduce the risk of data breaches while maintaining employees productivity.



We can help.

Verizon has the expertise and solutions to help you strengthen

Talk to us about securing your enterprise today.

The author of this content is a paid contributor for Verizon

mobile device security.

- Verizon Data Breach Investigations Report 2024
 - Verizon 2023 Mobile Security Index

⁶ Omdia, Business Mobile Collaboration Survey, 2023

Lookout Security Graph Data, January 1st-December 31st, 2022 Verizon Mobile Security Index 2024 ⁵ IBM Cost of a Data Breach Report 2024. Research conducted by Ponemon Institute

